ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT®

Journal of Algebra 259 (2003) 43–58

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Smith theory and Hecke operators

Avner Ash [1]

Boston College, Department of Mathematics, Carney Hall, Chestnut Hill, MA 02467, USA

Received 9 February 2001

Communicated by Efim Zelmanov

Abstract

Of the connections between the cohomology of arithmetic groups and representations of Galois groups, some are known and more are conjectured. This paper proves one of these conjectures for certain monomial Galois representations. Let p be a prime. We show that the representation of the absolute Galois group of $\mathbb{Q}$ induced from an $\overline{\mathbb{F}}_p^\times$-valued ray class character of the cyclotomic field $\mathbb{Q}(\zeta_p)$ is attached to a Hecke eigenclass in the mod p cohomology of a torsion-free congruence subgroup $\Gamma(M)$ of $GL(p-1,\mathbb{Z})$. The method involves constructing an action of the Hecke algebra on the fundamental exact sequence of Smith theory arising from the action by conjugation of an element of order p in $GL(p-1,\mathbb{Z})$ on $\Gamma(M)$.

0. Introduction

Let p be a prime number. In this paper we apply the key idea of Smith in his study of the action of a p-group on a topological space to a question in number theory. This question involves a conjecture that relates the mod p cohomology of arithmetic groups to mod p representations of Galois groups. The mediating object here is the algebra of Hecke operators acting on the group cohomology.

The idea to apply Smith theory stems from a paper of A. Adem [Ad] where he uses it to derive lower bounds for the Betti numbers of torsion-free congruence groups. Our

E-mail address: avner.ash@bc.edu.

[1] Research partially supported by NSA grant MDA 904-00-1-0046, for which I gratefully thank the NSA. This manuscript is submitted for publication with the understanding that the United States government is authorized to reproduce and distribute reprints.

0021-8693/02/$ – see front matter
PII: S0021-8693(02)00547-1

innovation is to impose an action of the Hecke algebra on the Smith exact sequence. In this way we are able to prove a conjecture stated in [AS] in some special cases.

This conjecture generalizes a well-known conjecture of Serre's [Se]. Our conjecture states that given a mod-p n-dimensional "odd" Galois representation ρ of the Galois group $G_{\mathbb{Q}}$ of an algebraic closure of $\mathbb{Q}$ over $\mathbb{Q}$ there exists a mod-p cohomology class f "attached" to ρ. The Hecke polynomial is built from the Hecke eigenvalues on f. The meaning of "attached" may be found in Definition 0.1 below.

In this paper we prove the conjecture when ρ is induced from a ray class character of the cyclotomic field of pth roots of unity. Thus $n = p - 1$ and p is any prime number > 2.

From now on let p be an odd prime and $\mathbb{F}$ a fixed algebraic closure of $\mathbb{Z}/p$. If $\eta : (\mathbb{Z}/M)^{\times} \to \mathbb{F}^{\times}$ is a character, we denote by $\mathbb{F}_{\eta}$ the one-dimensional module on which $GL(n, \mathbb{Q}_{(M)})$ acts via $\eta \circ \det$.

Most homology and cohomology groups below will be taken with trivial $\mathbb{F}$ coefficients, in which case we will omit the coefficient module from the notation.

Fix $n \geqslant 2$, and Γ to be the group $SL(n, \mathbb{Z})$. Fix a positive integer M, let $S_M(M)$ be the subsemigroup of the integral matrices x in $GL(n, \mathbb{Q})$ such that the determinant of x is positive and prime to M, and x is congruent to the diagonal matrix $\operatorname{diag}(1, \ldots, 1, *)$ modulo M. Let $\Gamma(M) = \Gamma \cap S_M(M)$ be the principle congruence subgroup of level M. Then $(\Gamma(M), S_M(M))$ is a congruence Hecke pair of level M in the sense of [A]. Note that $\Gamma(M)$ is torsion-free as soon as $M > 2$.

The $\mathbb{F}$-algebra of double cosets $\Gamma(M)\backslash S_M(M)/\Gamma(M)$ is denoted by $\mathcal{H}$. In particular, it contains all double cosets of the form $\Gamma(M)D(l,k)\Gamma(M)$, where $D(l,k)$ is a diagonal matrix in $S_M(M)$ such that $\Gamma D(l,k)\Gamma = \Gamma \operatorname{diag}(1, \ldots, 1, l, \ldots, l)\Gamma$ with k 1's followed by $(n-k)$ l's, and l is a prime not dividing M. We let $T(l,k)$ denote this double coset, viewed as a Hecke operator.

As reviewed in [A], $\mathcal{H}$ acts on the homology and cohomology of $\Gamma(M)$ in a way which generalizes the classical action of Hecke operators on the cohomology of the modular curves. One of the main interests of this action is its link with non-Abelian reciprocity laws in Galois theory.

Definition 0.1. Let $\mathcal{V}$ be an $\mathcal{H}$-module and suppose $v \in \mathcal{V}$ is an eigenclass for the action of $\mathcal{H}$ with $T(l,k)v = a(l,k)v$ for some $a(l,k) \in \mathbb{F}$ for all $k = 0, \ldots, n$ and all l prime to M. Let ρ be a continuous semisimple representation $\rho : G_{\mathbb{Q}} \to GL(n, \mathbb{F})$ unramified outside pM such that

$$\sum_k (-1)^k l^{k(k-1)/2} a(l,k) X^k = \det\bigl(\bigl(I - \rho(\mathrm{Frob})_l\bigr)^{-1} X\bigr)$$

for all l not dividing pM. Then we shall say that ρ is attached to v.

When ρ is attached to v, many of the number theoretical properties of the fixed field of the kernel of ρ can be read off from the Hecke eigenvalues of v and vice versa. This is why we call such a relationship a non-Abelian reciprocity law. One of the most important properties of either ρ or v is its sheer existence. Putting together the conjectures of [A,AS] we obtain the following conjecture that ρ's and v's "predict" each other. First, define ρ

to be “odd” if the number of $+1$ eigenvalues of ρ (complex conjugation) and the number of its -1 eigenvalues differ by at most 1. (Warning: this is different from the definition of “odd” in [ADP].)

Conjecture 0.2. (a) *Any $\mathcal{H}$-eigenclass in $H^*(\Gamma(M), \mathbb{F}_\eta)$ has some $\rho : G_\mathbb{Q} \to GL(n, \mathbb{F})$ attached.*

(b) *Conversely given an odd ρ, then there exist some M and η such that ρ is attached to some $\mathcal{H}$-eigenclass in $H^*(\Gamma(M), \mathbb{F}_\eta)$.*

Remark. In [A] no mention was made of “oddness” but I now believe that (a) should be supplemented by the assertion that the attached ρ be odd.

For the status of this conjecture, see [AS,ADP]. Basically, (a) is known for $n = 1, 2$ and (b) is known for $n = 1$. There has been some very interesting recent work on (b) for $n = 2$ by Richard Taylor and his coworkers. See for example [B1,S-BT,T1,T2]. For $n = 3$ there is some computer evidence for both (a) and (b), but for $n > 3$ there is very little known about either part. As stated above, the purpose of this paper is to prove (b) for a certain family of monomial ρ's where n can be arbitrarily large. Note that the ρ's in Theorem 1.1 are generally irreducible.

This family of Galois representations has appeared before in conjunction with Farrell cohomology in [A,A1]. The Farrell cohomology of $GL(p-1, \mathbb{Z})$ with mod p coefficients is especially easy to describe. It relies on the existence of p-torsion in the group, and since the group contains no $\mathbb{Z}/p \times \mathbb{Z}/p$ it is easy to compute algebraically. However, Farrell cohomology vanishes for torsion-free groups. Also, unlike ordinary cohomology, it is not obviously related to automorphic forms or the cohomology of arithmetic locally symmetric spaces.

In the current paper, given ρ, the desired Hecke eigenclasses to which ρ is attached will be found in the *usual* group cohomology of a torsion-free principle congruence subgroup. It is hoped the Smith-theoretic method here can be extended to other cases of the conjecture.

1. Statement of the main theorem

Let ζ be a fixed primitive pth root of 1 and set $L = \mathbb{Q}(\zeta)$. Let E be the ray class group of L of conductor M. Consider a character $\theta : E \to \mathbb{F}^\times$, of conductor dividing M. Because the target has no p torsion, we see without loss of generality that we can and will assume that p divides M exactly once. By class field theory we can view θ as a character of the absolute Galois group G_L of G.

We write $M = pN$ where p is prime to N. Note that since p is odd, $\Gamma(M)$ is torsion-free and $H^*(\Gamma(M)) = 0$ if $* > n(n-1)/2 =$ the cohomological dimension of $\Gamma(M)$ by [BS].

We state our main theorem here, and prove it in a slightly different but equivalent form as Theorem 4.5 in Section 4.

Theorem 1.1. *Let θ be as above and let $\rho = \mathrm{Ind}(G_L, G_{\mathbb{Q}}, \theta)$, so $n = p - 1$. Then there exists a character $\eta : (\mathbb{Z}/M)^\times \to \mathbb{F}^\times$ and a $\beta \in H^*(\Gamma(M), \mathbb{F}_\eta)$ which is an eigenclass for the action of the Hecke algebra $\mathcal{H}$ such that ρ is attached to β.*

We can remove p from the level:

Corollary 1.2. *Given ρ and η as in the theorem, there exists an irreducible $\mathbb{F}[GL_n(\mathbb{Z}/p)]$-module W (on which $S_N(N)$ acts via reduction mod p), and a Hecke eigenclass α in $H^*(\Gamma(N), W \otimes \mathbb{F}_\eta)$ such that ρ is attached to α.*

Proof. By Shapiro's lemma (see [AS1]) we have an isomorphism of Hecke modules:

$$H^*\big(\Gamma(M), \mathbb{F}_\eta\big) \approx H^*\big(\Gamma(N), \mathrm{Ind}\big(1, SL_n(\mathbb{Z}/p), \mathbb{F}_\eta\big)\big).$$

The corollary now follows easily as in the proof of Lemma 2.1 in [AS1]. $\square$

Idea of the proof of Theorem 1.1: We can (and will) work with homology since it is algebraically dual to cohomology. Let π be an element of order p in $\Gamma := SL(n, \mathbb{Z})$. (Remember, $n = p - 1$.) We form a finite-dimensional $B\Gamma(M)$-space X and perform the Smith construction on its singular chains, using π. A convenient reference for this construction is [B, Chapter III, Section 3].

We then define an $\mathcal{H}$-action on the chains so that the Smith exact sequence becomes an exact sequence of $\mathcal{H}$-modules. We study carefully the fixed-point set X^π which appears in the Smith exact sequence, and we construct a nonzero element in its homology which is an eigenvector for $\mathcal{H}$ modulo the Smith homology group to which it is tied. The system of Hecke eigenvalues appearing on this element has ρ attached. Then the key idea of Smith theory allows us to lift the desired system of Hecke eigenvalues to the homology of X, which is the same as the homology of $\Gamma(M)$.

To work easily with the Hecke operators, it will be convenient to use a double-coset adelic space for X, as is done in the theory of automorphic representations. So X will actually be a finite union of $B\Gamma(M)$-spaces. At the end of Section 4 we make the necessary comparison between the adelic Hecke operators and the "classical" ones.

2. Smith exact sequence

The material in this section is easily generalized as follows: G can be replaced by an arbitrary reductive group defined over $\mathbb{Z}$, $\Gamma(M)$ by a torsion-free arithmetic subgroup of $G(\mathbb{Z})$, and π by an element of order p in $G(\mathbb{Z})$. For simplicity, we will stick to the case at hand.

We introduce the following notation. As above, p is an odd prime and $n = p - 1$. We set $G = GL_n$, $Z =$ the center of G. Let $\mathbb{A}$ be the adeles of $\mathbb{Q}$. We embed $\mathbb{Q}$ into $\mathbb{A}$ diagonally: $a \mapsto (a, a, a, \ldots)$. If $a \in \mathbb{Q}$ and v is any place of $\mathbb{Q}$, $a_v = (1, \ldots, 1, a, 1, \ldots) \in \mathbb{A}$ with a in the vth place. If $M \geqslant 2$ we set $a_M = \prod_{v|M} a_v$. Also, $a_f = \prod_{v \neq \infty} a_v$. We use similar notation for other adelic objects. Note that $\mathbb{A}_f$ is a totally disconnected space, so that the connected component of any point is itself.

Continue with notation: for any prime l, $K_l = G(\mathbb{Z}_l)$, $K_l(l^e) = \{g \in K_l \mid g \equiv 1 \bmod (l^e)\}$. Then by our conventions, $K_M = \prod_{l|M} K_l$. We set $K_M(M) = \prod_{l^e \| M} K_l(l^e)$.

Now we construct the locally symmetric space. We define $K_\infty = O(n)$, $X_\infty = G_\infty / Z_\infty K_\infty$, and $K_f(M) = \prod_{l \nmid M} K_l \times K_M(M)$. Finally, we set $X(M) = G(\mathbb{Q}) \backslash G(\mathbb{A}) / Z_\infty \times K_\infty K_f(M) = G(\mathbb{Q}) \backslash X_\infty \times G(\mathbb{A}_f)/K_f(M)$. When M is understood we will just write K_f and X.

If S is any subset in a coset space that projects naturally down to $X(M)$, let $\overline{S}$ denote its image in $X(M)$.

One knows that $X(M) \approx \coprod_{(\mathbb{Z}/M)^\times} \Gamma(M) \backslash X_\infty$, or more exactly, $X(M) = \coprod \overline{X_\infty y_d}$ where $y_d = \mathrm{diag}(1, \ldots, 1, d)_M$ and d runs through a set of representatives in $\mathbb{Z}$ for $(\mathbb{Z}/M)^\times$. (The basic point of the proof is that the reduction map $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/M)$ is surjective.)

Recall that N denotes a positive integer prime to p, $M = pN$ and $X = X(M)$. Then X is a finite-dimensional manifold of dimension $D = n(n+1)/2 - 1$ with $\phi(M)$-connected components. Since $p \geqslant 3$, $\Gamma(M)$ is torsion-free.

For any topological space Y, Let $C_*^+(Y)$ be the singular chains on Y with coefficients in $\mathbb{F}$. This is the free $\mathbb{F}$-module spanned by continuous maps $\sigma : \Delta_* \to Y$ where Δ_* is the standard $*$-dimensional simplex.

When Y is a subspace of X, we truncate this chain complex as follows: Set $C_*(Y) = C_*^+(Y)$ if $* \leqslant D$, $C_{D+1}(Y) = \mathrm{Ker}(\partial : C_D \to C_{D-1})$, and $C_*(Y) = 0$ if $* > D+1$. Then the homology of $C_*(X)$ equals the direct sum of $\phi(M)$ copies of the homology of $\Gamma(M)$ with trivial $\mathbb{F}$ coefficients.

Let $\mathcal{O}$ be the ring of integers in L. Let π be the matrix of order p in Γ that represents multiplication by ζ on the basis $B_0 = (\zeta, \zeta^2, \ldots, \zeta^n)$. Thus π is the companion matrix of the cyclotomic polynomial $X^{p-1} + X^{p-2} + \cdots + 1$.

More generally, the basis B_0 defines an embedding of $\mathbb{Q}$-algebras $L \to M_n(\mathbb{Q})$ so that $L^\times \to G(\mathbb{Q})$ and $\mathcal{O} \to G(\mathbb{Z})$. If $x \in L$, we will denote by $\tilde{x}$ its image in $G(\mathbb{Q})$.

Now π_M acts on the right on X, since $K_M(M)$ is normal in K_M. Note that π_f and π_M have the same effect on X since $\pi_l \in K_l$ for all $l \nmid M$. Then π_M also acts on $C_*(X)$ on the right.

A simplex σ is either (a) fixed by π_M (if and only if its image lies in the fixed-point set X^{π_M}) or (b) the group P generated by π_M acts freely on the orbit σP.

We now define an action of the Hecke Algebra on $C_*(X)$ that will descend to the usual Hecke action on homology and cohomology. For $l \nmid M$, let $s = \mathrm{diag}(1, \ldots, 1, l, \ldots, l) \in G(\mathbb{Q})$. Choose coset representatives $s_i \in G(\mathbb{Q})$ so that

$$K_l s_l K_l = \coprod s_{i,l} K_l.$$

If σ is any simplex, lift it to a continuous map $\sigma_0 : \Delta_* \to X_\infty \times G(\mathbb{A}_f)/\prod_{r \nmid lM} K_r \times K_M(M)$. Then set

$$\sigma T_s = \sum_i \overline{\sigma_0 s_{i,l}}.$$

One checks easily that (1) this is independent of the choices of σ_0 and $\{s_i\}$, (2) it works on $C_{D+1}(X)$ just as well, since $C_{D+1}(X)$ is generated by boundaries of $(D+1)$-dimensional simplices, (3) it commutes with the boundary maps, and (4) it commutes with π_M.

Now fix c, $1 \leqslant c \leqslant p-1$, and set $\beta = (1-\pi)^c$, $\beta' = (1-\pi)^{p-c}$, so $\beta, \beta' \in \mathbb{F}[\pi]$.

Lemma 2.1. *We have an exact sequence of $\mathcal{H}$-modules*:

$$0 \to C_*(X)\beta_M \oplus C_*\bigl(X^{\pi_M}\bigr) \to C_*(X) \to C_*(X)\beta'_M \to 0$$

where the last nonzero map is multiplication by β'_M on the right.

Proof. First prove this for $C_*^+(X)$ in place of $C_*(X)$. The proof is standard—see, e.g., [B, Theorem 3.1, pp. 122–123]. A simple diagram chase verifies it also for C_{D+1}, using the fact that $C_{D+1} = \operatorname{Im} \partial_{D+1}^+ = \operatorname{Ker} \partial_D^+$, where ∂_*^+ denotes the boundary map in the C_*^+ sequence. □

We define the Smith homology groups by $H_*^{\beta}(X) = H_*(C_*(X)\beta_M)$ and similarly for $H_*^{\beta'}(X)$. Since the right action of π_M and hence of β_M and β'_M commute with the Hecke operators T_s, $\mathcal{H}$ acts on the Smith homology groups and also on $H_*(\operatorname{Ker}(\beta'_M)) = H_*^{\beta}(X) \oplus H_*(X^{\pi_M})$. However, we are not asserting that $H_*(X^{\pi_M})$ itself is stable under $\mathcal{H}$, although of course $H_*(X)^{\pi_M}$ is.

Lemma 2.2. *We have a long exact sequence of $\mathcal{H}$-modules*:

$$\cdots \to H_{*+1}^{\beta'}(X) \to H_*^{\beta}(X) \oplus H_*\bigl(X^{\pi_M}\bigr) \to H_*(X) \to H_*^{\beta'}(X) \to \cdots.$$

Proof. From Lemma 2.1, we immediately get a long exact sequence of homology groups. It is easy to check that all the maps, including the boundary maps, are $\mathcal{H}$-equivariant. □

Remark. We can define Smith cohomology groups by taking the homology of the cocomplex $\operatorname{Hom}(C_*(X)\beta_M, \mathbb{F})$. Defining Hecke actions to be the adjoints of those on homology, we get an analogous long exact sequence in cohomology.

3. A lifting lemma in linear algebra

Let k be a field, R a commutative k-algebra, B an R-module. Let $B_1 \subset B$ be an R-submodule, $b \in B - B_1$, and $\chi : R \to k$ a k-homomorphism such that $rb \in \chi(r)b + B_1$ for all $r \in R$. We will call (b, B_1) a "one-dimensional subquotient of B with character χ."

Lemma 3.1. *Let $A \xrightarrow{f} B \xrightarrow{g} C$ be an exact sequence of R-modules. If B contains a one-dimensional subquotient with character χ then so does either A or C.*

Proof. Let (b, B_1) be a one-dimensional subquotient of B with character χ. If $g(b) \notin g(B_1)$ then $(g(b), g(B_1))$ is the desired one-dimensional subquotient of C. If $g(b) = g(b_1)$

for some $b_1 \in B_1$, replacing b by $b - b_1$, we may assume $g(b) = 0$. Then pick $a \in A$ such that $f(a) = b$. Claim: $(a, f^{-1}(B_1))$ is the desired one-dimensional subquotient of A. Clearly $a \notin f^{-1}(B_1)$ since $b \notin B_1$. And for any $r \in R$, $f(ra) = rb = \chi(r)b + b_2$ for some $b_2 \in B_1$ so $f(ra - \chi(r)a) = b_2 \in B_1$. In other words, $ra \in \chi(r)a + f^{-1}(B_1)$. □

Let $B \neq (0)$ be an R-module which is finite dimensional over k. For any $r \in R$, let B_r be the $\chi(r)$-generalized eigenspace of B for r acting on B, and let B_r' be the sum of all the other generalized eigenspaces for r, so $B = B_r \oplus B_r'$.

Lemma 3.2. *Let B be as in the preceding paragraph. If $B = B_r$ for all $r \in R$ then B contains a χ-eigenvector.*

Proof. By induction on $\dim_k(B)$, the one-dimensional case being obvious. If, for all $r \in R$, $(r - \chi(r))B = 0$, any nonzero vector of B works. Otherwise, let $s \in R$ be such that $0 \neq (s - \chi(s))B$. We also know that $(s - \chi(s))B \neq B$ since B must contain a $\chi(s)$-eigenvector for s (because $B = B_s$). Let $C = (s - \chi(s))B$. Then $C_r = C$ for all $r \in R$, so we are done by induction. □

Lemma 3.3. *Let B be an R-module, finite dimensional over k, which contains a one-dimensional subquotient (b, B_1) with character χ. Then B contains a χ-eigenvector.*

Proof. By induction on $\dim_k(B)$, the one-dimensional case being obvious. If $B = B_r$ for all $r \in R$ we are done by the preceding lemma. If $B \neq B_s$ for some $s \in R$, consider the exact sequence

$$0 \to B_s' \to B \to B_s \to 0.$$

Let $\bar{b}$, $\overline{B_1}$ be the projections into B_s. If $\bar{b} \in \overline{B_1}$, then by the proof of Lemma 3.1 there exists a one-dimensional subquotient of B_s' with character χ. But that is impossible (using the induction hypothesis) since $\chi(s)$ does not appear as an eigenvalue on B_s'. Therefore, $\bar{b} \notin \overline{B_1}$ and $(\bar{b}, \overline{B_1})$ is a one-dimensional subquotient with character χ in B_s. We are finished now by induction. □

4. Application to the Smith exact sequence

Lemma 4.1. *If for some $j \geqslant 0$ the $\mathcal{H}$-module $H_j^{\beta}(X) \oplus H_j(X^{\pi_M})$ contains a one-dimensional subquotient with character χ, then so does $H_*(X)$ for some $*$, $j \leqslant * \leqslant n(n-1)/2$.*

Proof. Consider Lemma 2.2. If the given subquotient maps nonzero to $H_j(X)$ we are finished. If not, then by Lemma 3.1, such a subquotient exists in $H_{j+1}^{\beta'}(X)$. We now write down the long exact sequence of Lemma 2.2 but with β and β' switched. Then we repeat the argument with $j + 1$. This process must stop because C_* is 0 above dimension $D + 1$. Thus we obtain a one-dimensional subquotient with character χ in $H_*(X)$ for some $*$,

$j \leqslant *$. Since the homology of $\Gamma(M)$ and hence that of X vanishes above dimension $n(n-1)/2$ [BS], this proves the lemma. □

Let θ be a ray class character as in Section 1 and let $\rho_\theta = \mathrm{Ind}(G_L, G_{\mathbb{Q}}, \theta)$. We are now going to define a particular character χ_θ with the property that ρ_θ is attached to any $\mathcal{H}$-eigenvector with eigencharacter χ_θ.

For each $l \nmid M = pN$, factor $l\mathcal{O} = \mathcal{L}_1 \cdots \mathcal{L}_{n/d}$ where d is the degree of l in L. Let $\mathcal{I}$ denote the set of subsets of $\{1, \ldots, n/d\}$ with exactly k/d elements. In particular, if $d \nmid k$, then $\mathcal{I}$ is the empty set. For each $Q \in \mathcal{I}$, let e_Q denote the class of the ideal $\lambda_Q = \prod_{i \in Q} \mathcal{L}_i$ in the ray class group E of level M.

Define $\chi_\theta : \mathcal{H} \to \mathbb{F}$ by $\chi_\theta(T_{l,k}) = \sum_{Q \in \mathcal{I}} \theta(e_Q)$.

Lemma 4.2. *Any $\mathcal{H}$-eigenvector with eigencharacter χ_θ has ρ_θ attached.*

Proof. This follows immediately from [A, Theorem 6.1.2] upon composing the equality in that theorem with the homomorphism θ. □

Theorem 4.3. *Let θ be as above. Then there exists an $(\mathcal{H}-1)$-dimensional subquotient with character χ_θ in $H_*^\beta(X) \oplus H_*(X^{\pi_M})$.*

Applying Lemmas 3.3, 4.1, and 4.2 to Theorem 4.3 we obtain:

Corollary 4.4. *Let θ be as above. Then there is an $\mathcal{H}$-eigenvector α in $H_*(X)$ with ρ_θ attached.*

It is now an easy exercise to compare the "classical" Hecke operators on group homology to our adelic operators to prove Theorem 1.1, which we restate here in terms of homology for convenience.

Theorem 4.5. *Let θ be as above and let $\rho = \mathrm{Ind}(G_L, G_{\mathbb{Q}}, \theta)$, so $n = p-1$. Then there exists a character $\eta : (\mathbb{Z}/M)^\times \to \mathbb{F}^\times$ and a $\beta \in H_*(\Gamma(M), \mathbb{F}_\eta)$ which is an eigenclass for the action of the Hecke algebra $\mathcal{H}$ such that ρ is attached to β.*

Proof. We begin by fixing homeomorphisms between the connected components of X. Recall that $X = \coprod \overline{X_\infty y_d} = \coprod C_d$ where $y_d = \mathrm{diag}(1, \ldots, 1, d)_M$ and d runs through a set of representatives in $\mathbb{Z}$ for $(\mathbb{Z}/M)^\times$. Then right multiplication by y_d defines our desired homeomorphism $C_k \to C_{dk}$. In fact, since X is right invariant under $K_M(M)$, we actually get a group action of $(\mathbb{Z}/M)^\times$ on X via $d \mapsto$ right multiplication by y_d.

In the definition of the action of $\mathcal{H}$ we have to choose the coset representatives s_i. From [A, Lemma 1.1.(a)] we see that we can always assume that $s_i \equiv \mathrm{diag}(1, \ldots, 1, *) \bmod M$ for all i. Denote by $\widehat{T}_s$ the classical Hecke operator acting on $H_*(\Gamma(M), \mathbb{F})$. Then it is easy to see that if $\alpha = \sum \alpha_d$ is in $H_*(X) = \bigoplus H_*(C_d)$ then

$$\widehat{T}_{s^{-1}}(\alpha_{d(\det s^{-1})}) = (T_s\alpha)_d.$$

Apply this to the α in Corollary 4.4. Let us abbreviate $\chi_\theta(T_s) = b(s)$. Then we have $(T_s\alpha) = b(s)\alpha$ for all s. It follows that

$$\widehat{T}_s(\alpha_d) = b(s)\alpha_{d(\det s^{-1})}.$$

Now the $(\mathbb{Z}/M)^\times$-action on $H_*(X)$ commutes with $\mathcal{H}$, so consider the $\mathbb{F}[(\mathbb{Z}/M)^\times]$-span of α. Since $(\mathbb{Z}/M)^\times$ is commutative, this span contains an eigenelement with eigencharacter $\psi : (\mathbb{Z}/M)^\times \to \mathbb{F}^\times$ say. Without loss of generality, we may assume that α is this eigenelement. Then $\alpha_{c^{-1}d} = \psi(c)\alpha_d$ for all $c, d \in (\mathbb{Z}/M)^\times$. Hence $\widehat{T}_s(\alpha_d) = b(s)\psi(s)\alpha_d$.

Since $\alpha \neq 0$, there is some d for which $\alpha_d \neq 0$. Then we may take $\beta = \alpha_d$ viewed as an element in $H_*(\Gamma(M), \mathbb{F}_\eta)$, where $\eta = \psi^{-1}$. $\square$

The remainder of the paper will be occupied with proving Theorem 4.3.

5. Connected components of the fixed-point set

Recall that E denotes the ray class group of L of conductor M. Let E_P denote the subgroup generated by the classes of the principle ideals. Then we have an exact sequence

$$0 \to E_P \to E \to C \to 0$$

where C is the absolute class group of L. We also know that $E_P \approx Y_M/U_M$ where $Y_M = (\mathcal{O}/M\mathcal{O})^\times$ and U_M is the image of $\mathcal{O}^\times$ in Y_M.

We want to define an action of E on a certain subset of the set of connected components $\pi_0(X^{\pi_M})$ of X^{π_M}.

First we have to review some facts about the elements of order p in $G(\mathbb{Z})$ which follow from [CR, Theorem 34.31, p. 729]. Let I be an ideal in $\mathcal{O}$, with a $\mathbb{Z}$-basis $B = (b_1, \ldots, b_n)$ for it. Define the matrix π_B by

$$\zeta B_I = (\zeta b_1, \ldots, \zeta b_n) = B\pi_B.$$

Every matrix of order p in $G(\mathbb{Z})$ is equal to π_B for some I and choice of basis B. If we change the basis, this has the effect of conjugating π_B within $G(\mathbb{Z})$. In case $I = \mathcal{O}$, we will always take $B = B_0 = (\zeta, \ldots, \zeta^n)$ so that $\pi_B = \pi$.

Later we will fix a set of ideals $\{I\}$ including $\mathcal{O}$ which represent the elements of C. For each I we will fix a basis B_I, and set $\pi_I = \pi_{B_I}$. Then $\{\pi_I\}$ will run through a set of representatives for the conjugacy classes of elements of order p in Γ.

Lemma 5.1. *If $\phi \in G(\mathbb{Z})$ has order p then ϕ is conjugate to some $\phi' \in G(\mathbb{Z})$ such that there exists a matrix $m \in G(\mathbb{Q}_{(M)})$ such that* $\det(m) \equiv 1 \bmod M$ *and $\phi' = m\pi m^{-1}$. In particular, $\phi' \equiv \pi \bmod M$.*

Proof. As stated above, we may take $\phi = \pi_B$ for some I and choice of basis $B = (b_1, \ldots, b_n)$. If g is the change of basis matrix whose columns are the coordinates of $b_1, \ldots, b_n$ with respect to B_0, then $g \in M_n(\mathbb{Z})$, $\det(g) = \mathrm{Norm}(I)$, and $g\pi g^{-1} = \pi_B$.

Sublemma 5.2. *In any ideal class $\kappa \in C$ there exist infinitely many ideals I with* $\mathrm{Norm}(I) \equiv 1 \bmod M$.

Proof of sublemma. We shall show there are infinitely many prime numbers A with $A \equiv 1 \bmod M$ such that some prime ideal in $\mathcal{O}$ over A lies in κ.

Let H be the Hilbert class field of L, so $\mathrm{Gal}(H/L) \approx C$ and H is unramified everywhere over L. Let $G_1 = \mathrm{Gal}(H/\mathbb{Q})$, so $C \subset G_1$. Let ζ_N be a primitive Nth root of unity and $G_2 = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Since $H/\mathbb{Q}$ is ramified only at p and $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ only away from p, they are disjoint extensions and $\mathrm{Gal}(H(\zeta_N)/\mathbb{Q}) \approx G_1 \times G_2$. By Chebotarev density, there are infinitely many primes A not dividing $pN = M$ such that Frob_A is in the conjugacy class of $(\kappa, 1) \in G_1 \times G_2$. Any such A has our desired properties. □

Back to $\phi = \pi_B$. By the sublemma we see that by changing I within its ideal class, we may assume we have $g \in M_n(\mathbb{Z})$, $\det(g) \equiv 1 \bmod M$ and $g\pi g^{-1} = \pi_B$. Let $h \in SL_n(\mathbb{Z})$ be such that $h \equiv g \bmod M$. Then $\pi_{Bh} = h^{-1}\pi_B h = h^{-1} g \pi_B (h^{-1}g)^{-1} \equiv \pi \bmod M$. So we can take $\phi' = \pi_{Bh}$. □

Recall the embedding $L \to M_n(\mathbb{Q})$ via the basis B_0, $x \mapsto \tilde{x}$. This embedding induces an embedding $Y_M \to G(\mathbb{Z}/M) = K_M/K_M(M)$ which we also denote by $\tilde{\ }$. In this way Y_M acts on X on the right. Since Y_M commutes with π_M, it also acts on X^{π_M} and hence on $\pi_0(X^{\pi_M})$.

Also recall that $X = \coprod \overline{X_\infty y_d}$ is the decomposition of X into connected components. In particular, one of them is $\overline{X_\infty} \approx \Gamma(M)\backslash X_\infty$. For any invertible matrix m let $\langle m \rangle$ denote the group generated by m.

Lemma 5.3. $\overline{X_\infty} \cap X^{\pi_M} = \coprod \overline{X_\infty^{\phi_\infty}}$ *where $\langle \phi \rangle$ runs through a set of representatives of subgroups of order p in $G(\mathbb{Z})$ such that $\langle \phi \rangle \equiv \langle \pi \rangle \bmod M$ modulo conjugation by $\Gamma(M)$. Moreover, $\overline{X_\infty^{\phi_\infty}} \approx N_\phi \backslash X_\infty^{\phi_\infty}$, where N_ϕ denotes the normalizer in $\Gamma(M)$ of $\langle \phi \rangle$ embedded into G_∞.*

Proof. This follows from [Br, p. 267]. See also [Ad, p. 725]. □

Remark. It is crucial here that $\Gamma(M)$ be torsion-free.

The following lemma is easy to establish, so its proof will be omitted.

Lemma 5.4. *If R is any commutative ring with identity, let $\hat{\pi}$ be the image of π in $G(R)$ under the map induced the natural map $\mathbb{Z} \to R$. If $f \in G(R)$ commutes with $\hat{\pi}$ then there exists a polynomial $a(T) \in R[T]$ such that $f = a(\hat{\pi})$.*

We denote by ξ the image of $\overline{X_\infty^{\pi_\infty}}$ in $\pi_0(X^{\pi_M})$.

Lemma 5.5. $\mathrm{Stab}_{Y_M}\,\xi = U_M$.

Proof. Let $y \in Y_M$ such that $\xi = \xi y = \xi \tilde{y}_M$. Then y also fixes the connected component $\overline{X}_\infty$ of X and therefore $\det y \equiv 1 \bmod M$.

Let $g \in SL_n(\mathbb{Z})$ be such that $g \equiv y \bmod M$. Then $\xi = \xi y^{-1} = \xi g_M^{-1}$ implies that $X_\infty^{(g\pi g^{-1})_\infty} = g_\infty X_\infty^{\pi_\infty}$ and $X_\infty^{\pi_\infty}$ have the same images in $\Gamma(M)\backslash X_\infty$. By Lemma 5.3, it follows that $\langle\pi\rangle$ and $\langle g\pi g^{-1}\rangle$ are conjugate by an element of $\Gamma(M)$. Multiplying g by that element we may assume that $\langle\pi\rangle = \langle g\pi g^{-1}\rangle$. But g and π commute mod M, so in fact $\pi = g\pi g^{-1}$. Then by Lemma 5.4, g is a polynomial in π with integral coefficients, and since g has determinant 1, it follows that $g = \tilde{u}$ for some $u \in \mathcal{O}^\times$. Hence $y \in U_M$. $\square$

Thus $E_P \approx Y_M/U_M$ acts on ξY_M. We want to extend this to an action of E. Write X_0 for the connected component $\overline{X}_\infty$ of X. Then $X^{\pi_M} \cap X_0 = X_0^{\pi_M}$. Set $X_M = X_0^{\pi_M} Y_M$. We will define an action of E on $\pi_0(X_M)$ and later on $H_*(X_M)$.

If I is an fractional ideal in L prime to M let $[I]$ denote its class in E and $[\![I]\!]$ its class in C. We fix once for all a set $\mathcal{R}$ of representatives $I_1, \dots, I_h$ for the classes in C such that $\mathrm{Norm}\, I_j \equiv 1 \bmod M$ for all j. For each I we fix a $\mathbb{Z}$-basis B_I such that $\zeta B_I = B_I \pi_I$ with a matrix $\pi_I \in G(\mathbb{Z})$ of order p and such that the change of basis matrix from B_0 to B_I is congruent to the identity mod M. In particular, $\pi_I \equiv \pi \bmod M$. We choose $I_1 = \mathcal{O}$ and $B_{\mathcal{O}} = B_0$, so $\pi_{\mathcal{O}} = \pi$.

Set $\xi_I =$ image of $\overline{X_\infty^{\pi_{I\infty}}}$ in $\pi_0(X_0)^{\pi_M}$. Then $\pi_0(X_M) = \{\xi_I y \mid I \in \mathcal{R}, y \in Y_M\}$.

Definition 5.6. Given an ideal $\mathfrak{a}$ prime to M, so that $[\mathfrak{a}] \in E$, write $[\![I\mathfrak{a}]\!] = [\![J]\!]$ for some $J \in \mathcal{R}$. Then write $(b) = JI^{-1}\mathfrak{a}^{-1}$ for some $b \in L^\times$ such that (b) is prime to M. Then set

$$(\xi_I y) \cdot [\mathfrak{a}] = \xi_J y \tilde{b}.$$

We will normally not write the dot.

It is straightforward to show that this is independent of the choices, and gives an action of E on the orbit ξE.

Lemma 5.7. *E acts simply transitively on $\pi_0(X_M)$.*

Proof. First, it is easy to check that $\xi_I[JI^{-1}] = \xi_J$. Thus to show the action is transitive, it suffices to show that every connected component of $X_0^{\pi_M}$ is of the form $\xi_I y$ for some $I \in \mathcal{R}$ and $y \in Y_M$.

To see this, start with a given component $\overline{X_\infty^{\phi_\infty}}$, where $\phi \in G(\mathbb{Z})$, ϕ has order p, and $\phi \equiv \pi \bmod M$. Then ϕ is conjugate to π_I in $G(\mathbb{Z})$ for some $I \in \mathcal{R}$. Say $\phi = \gamma^{-1}\pi_I\gamma$ with $\gamma \in G(\mathbb{Z})$. Denoting reduction mod M by an overline, we have $\bar{\phi} = \bar{\pi}_I = \bar{\pi}$ and therefore $\bar{\gamma}$ centralizes $\bar{\pi}$. By Lemma 5.4, $\bar{\gamma} = a(\bar{\pi})$ for some polynomial $a(T) \in \mathbb{Z}[T]$. Set $y = a(\zeta)$. Note that since the determinant of γ is congruent to 1 mod M, so is the norm of y.

Write X_I for the connected component corresponding to ξ_I. Now I claim $\overline{X_\infty^{\phi_\infty}} = X_I y$. Indeed,

$$X_I y = X_I \gamma_M = \overline{\gamma_\infty^{-1} X_I} = \overline{X_\infty^{(\gamma^{-1}\pi_I\gamma)_\infty}} = \overline{X_\infty^{\phi_\infty}}.$$

Finally, we check the stabilizer of ξ_1 in E: Suppose $\xi_1 e = \xi_1$. Say $e = [\mathfrak{a}]$. Then since $I_1 = \mathcal{O}$, we have $[\![I_1]\!] = [\![I_1\mathfrak{a}]\!] = [\![\mathfrak{a}]\!]$ and therefore $\mathfrak{a}$ is principle. Say $\mathfrak{a} = (b)$. Then $\xi_1 b = \xi_1$ implies that $b \in \mathrm{Stab}_{Y_M}\,\xi_1 = U_M$ by Lemma 5.5. Hence $[\mathfrak{a}] = 1$ in E. $\square$

We now extend this to define an action of E on $H_*(X_M)$. Clearly, it suffices to define how an element of E acts on a single connected component, say the Ith one.

In the paragraphs before Lemma 5.6, we fixed representative ideals I with $\mathbb{Z}$-basis B_I such that the change of basis matrix $A_I \in G(\mathbb{Q}_{(M)})$ defined by the equation $B = B_0 A_I$ satisfies the congruence $A_I \equiv 1 \bmod M$. (We only need this congruence condition later, but it is well to keep it in mind.) Note that $\pi_I = A_I \pi A_I^{-1}$ so that

$$\pi_J = A_J A_I^{-1} \pi A_I A_J^{-1}.$$

Let $a_{IJ} = A_I^{-1} A_J$. By [A, Lemma 6.2.3(a)], the centralizer of any element ϕ of order p in $G(\mathbb{Z})$ is the set $\{f(\phi) \mid f \in \mathbb{Z}[T] \text{ and } f(\zeta) \in \mathcal{O}^\times\}$. It follows that conjugation by a_{IJ} sends the centralizer $Z_{\Gamma(M)}(\pi_J)$ isomorphically onto $Z_{\Gamma(M)}(\pi_I)$.

Now note that the normalizer and the centralizer of $\langle\phi\rangle$ in $\Gamma(M)$ are equal for any ϕ as above. Therefore, left multiplication by $a_{IJ,\infty}$ on X_∞ induces a homeomorphism from X_J to X_I. We can then define isomorphisms of cohomology groups denoted by the same letter $a_{IJ} : H_*(X_J) \to H_*(X_I)$.

Definition 5.8. Given an ideal $\mathfrak{a}$ prime to M, so that $[\mathfrak{a}] \in E$, write $[\![I\mathfrak{a}]\!] = [\![J]\!]$ for some $J \in \mathcal{R}$. Then write $(b) = JI^{-1}\mathfrak{a}^{-1}$ for some $b \in L^\times$ such that (b) is prime to M. Then if z is the homology class of a cycle $\sum n_\sigma \sigma$ in $C_*(X_I y)$, we define

$$z \cdot [\mathfrak{a}] = (a_{JI} z) y \tilde{b},$$

where the action of Y_M on homology is induced by its action on X.

This does not depend on the choices and does define an action because any matrix in $G(\mathbb{Q})_\infty$ which commutes with π_I will commute with its centralizer and therefore will act trivially on the homology of X_I.

For example, to see that nothing changes if we multiply b by a unit u in $\mathcal{O}^\times$ we need to check that $(a_{JI} z)\tilde{u} = (a_{JI} z)$. Write $u = f(\zeta)$ for some integral polynomial f. Recall that $\pi_J \equiv \pi \bmod M$, so $f(\pi_J) \equiv \tilde{u} \bmod M$. Then using the $G(\mathbb{Q})$-invariance of the adelic space on the left, we can bring $\tilde{u}$ from the right over to the left as $f(\pi_{J,\infty})$, where it acts trivially on $a_{JI} z$.

6. Computation of the Hecke operators

In this section we change the definition of Γ to $\Gamma = G(\mathbb{Z})$.

We now compute the Hecke operator T_s on $H_*(X_M)$, where $l \nmid M$, and $s = \mathrm{diag}(1, \ldots, 1, l, \ldots, l) \in G(\mathbb{Q})$, with k l's.

Recall that $l\mathcal{O} = \mathcal{L}_1 \cdots \mathcal{L}_{n/d}$ where d is the degree of l in L, $\mathcal{I}$ is the set of subsets of $\{1, \ldots, n/d\}$ with exactly k/d elements and for each $Q \in \mathcal{I}$, $\lambda_Q = \prod_{i \in Q} \mathcal{L}_i$.

Lemma 6.1. *Let $\mathfrak{a}$ be any fractional ideal in L prime to l with a $\mathbb{Z}$-basis $B = (b_1, \ldots b_n)$, and define the integral matrix ϕ of order p by $\zeta B = B\phi$. We have the isomorphism $\mathfrak{a} \approx \mathbb{Z}^n$ given by the basis B by sending $\sum m_j b_j$ to (m_j). Then we can choose coset representatives $\{s_i \in G(\mathbb{Q})\}$ so that $\Gamma s \Gamma = \coprod s_i \Gamma$, (so that also $K_l s_l K_l = \coprod s_{i,l} K_l$) and a partition of the cosets $\mathcal{D} = \{s_i \Gamma\} = \mathcal{D}_1 \amalg \mathcal{D}_2$ such that*

(a) $\mathcal{D}_1 = \{t\Gamma \in \mathcal{D} \mid t^{-1}\phi t \in \Gamma\}$;
(b) $\mathcal{D}_1 = \{t_Q \Gamma \mid Q \in \mathcal{I}\}$ *where $t_Q \in M_n(\mathbb{Z})$ is that matrix such that $\mathfrak{a}/\lambda_Q \mathfrak{a} \approx \mathbb{Z}^n / t_Q \mathbb{Z}^n$ via the isomorphism $\mathfrak{a} \approx \mathbb{Z}^n$ given by the basis B*; *and*
(c) $\langle \phi \rangle$ *acts freely on $\mathcal{D}_2$.*

Proof. Let t_Q be the matrix defined in (b). Claim: t_Q has elementary divisors $(1, \ldots, 1, l, \ldots, l)$, with k l's. Indeed, $(l) \subset \lambda_Q$ implies that $\mathfrak{a}/\lambda_Q \mathfrak{a}$ has exponent l. Therefore the elementary divisors of t_Q are $(1, \ldots, 1, l, \ldots, l)$, with some number of l's. How many? The index $[\mathfrak{a} : \lambda_Q \mathfrak{a}] = \mathrm{Norm}(\lambda_Q) = l^k$, so there are k of them.

Now $\mathfrak{a} = B\mathbb{Z}^n$ and $\lambda_Q \mathfrak{a} = Bt_Q \mathbb{Z}^n$. Therefore, Bt_Q is a basis for $\lambda_Q \mathfrak{a}$. Thus $B\phi t_Q = \zeta(Bt_Q) = (Bt_Q)\psi$ for some $\psi \in \Gamma$ of order p. In fact, we see that $t_Q^{-1}\phi t_Q = \psi \in \Gamma$.

Now I claim that the $t_Q \Gamma$ are pairwise distinct. We can view $\mathfrak{a}/\lambda_Q \mathfrak{a}$ as a k-plane in $\mathfrak{a}/l\mathfrak{a} \approx (\mathbb{Z}/l)^n$ which is ζ-stable. Then $t_Q \Gamma = t_R \Gamma$ implies that $\mathfrak{a}/\lambda_Q \mathfrak{a} = \mathfrak{a}/\lambda_R \mathfrak{a}$. But consider the $\langle \zeta \rangle$-module

$$(\mathbb{Z}/l)^n \approx \mathfrak{a}/l\mathfrak{a} \approx \prod_{j=1}^{n/d} \mathfrak{a}/\lambda_j \mathfrak{a}.$$

Each $\mathfrak{a}/\lambda_j \mathfrak{a}$ is distinguished by the d eigenvalues of ζ acting on it, since $\zeta, \ldots, \zeta^n$ remain distinct modulo l. Hence the same is true of the $\mathfrak{a}/l_Q \mathfrak{a}$. Thus we conclude that $\lambda_Q = \lambda_R$ and hence $Q = R$.

But we can now go backwards. The action of ϕ on $(\mathbb{Z}/l)^n$ is defined over the prime field $\mathbb{Z}/l$ so the eigenvalues of ϕ on any ϕ-stable subspace must be a union of orbits of Frob_l, which correspond exactly to the eigenvalues of ζ on the subspaces of $\mathfrak{a}/l\mathfrak{a}$ of the form $\mathfrak{a}/\mu\mathfrak{a}$ where μ runs over products of the λ_j's.

We apply this to show that if $t \in \Gamma s \Gamma$ and $t^{-1}\phi t \in \Gamma$ then $t\Gamma = t_Q \Gamma$ for some $Q \in \mathcal{I}$. First, $t^{-1}\phi t \in \Gamma$ implies that $\phi t = th$ for some $h \in \Gamma$. This implies that $\phi t \mathbb{Z}^n = t\mathbb{Z}^n$. Then ϕ stabilizes the subspace $\mathbb{Z}^n / t\mathbb{Z}^n \subset \mathbb{Z}^n / l\mathbb{Z}^n$ which must therefore be one of the above, corresponding to some μ. But since the determinant of t is l^k, this μ must be λ_Q for some $Q \in \mathcal{I}$, i.e., $t\mathbb{Z}^n = t_Q \mathbb{Z}^n$. It follows easily from this that $t\Gamma = t_Q \Gamma$.

We have now verified (a) and (b). For (c), let $t\Gamma \in \mathcal{D}_2$ and suppose $\phi t\Gamma = t\Gamma$. Then $\phi t = th$ for some $h \in \Gamma$. Then $t^{-1}\phi t \in \Gamma$ and $t\Gamma \in \mathcal{D}_1$, contradiction. $\square$

Recall that we have defined an action of the ray class group E on the homology of X_M, and that we denote the class of an ideal μ by $[\mu]$.

Theorem 6.2. *Fix an ideal $J \in \mathcal{R}$ and a number $y \in L$ such that (y) is prime to M. Let $w_\infty \tilde{y}_M$ be a cycle in the homology of $X_J \tilde{y}_M = \overline{X_\infty^{\pi_{J,\infty}} \tilde{y}_M}$. Then*

$$w_\infty T_s \equiv \sum_{Q\in\mathcal{I}} \overline{w_\infty \tilde{y}_M}[\lambda_Q] \quad \bmod C_*(X)\beta_M + \{\text{boundaries}\}.$$

Proof. Using the notation of Lemma 6.1, set $\mathfrak{a} = J$, so $\phi = \pi_J$ and use the decomposition $\mathcal{D} = \mathcal{D}_1 \amalg \mathcal{D}_2$ given by that lemma. Let t run through a set of representatives of the cosets in $\mathcal{D}$. Then

$$w_\infty T_s = \sum_t \overline{w_\infty \tilde{y}_M t_l}.$$

Group the terms as follows:

Case 1. If $t\Gamma \in \mathcal{D}_2$, take p terms $\phi^a t\Gamma \in \mathcal{D}_2$, where $a = 0, \dots, p-1$. Then

$$\sum_a \overline{w_\infty \tilde{y}_M(\phi^a t)_l} = \sum_a \overline{\left(t^{-1}\phi^{-a}\right)_\infty w_\infty \left(t^{-1}\phi^{-a}\right)_M \tilde{y}_M} = \sum_a \overline{\left[t_\infty^{-1} w_\infty t_M^{-1}\right]} \phi_M^{-a} \tilde{y}_M$$

because w_∞ is fixed pointwise by ϕ_∞.

Set x to be the term enclosed in square brackets in the last summation and write $x = x_1 + x_2 \in C_*(X^{\pi_M}) \oplus C_*(X)\beta_M$.

Then $\sum_a x_1\phi_M^{-a} = \sum_a x_1\pi_M^{-a} = 0$ since $\phi_M \equiv \pi_M \bmod M$, x_1 is fixed by π_M and we are in characteristic p.

Similarly, $\sum_a x_2\phi_M^{-a}\tilde{y}_M = \sum_a x_2\pi_M^{-a}\tilde{y}_M \in C_*(X)\beta_M$ since π and $\tilde{y}$ commute with $\beta = (1-\pi)^c$.

Case 2. Now suppose $t\Gamma \in \mathcal{D}_1$. Then $t\Gamma = t_Q\Gamma$ for some $Q \in \mathcal{I}$. We look now at the individual term

$$\overline{w_\infty \tilde{y}_M t_l} = \overline{t_\infty^{-1} w_\infty t_M^{-1} \tilde{y}_M}.$$

Now $t_\infty^{-1} w_\infty$ is a cycle in $\overline{X_\infty^{(t^{-1}\phi t)_\infty}}$.

Since $t\Gamma \in \mathcal{D}_1$, there is some $h \in G(\mathbb{Z})$ and some ideal $K \in \mathcal{R}$ such that $t^{-1}\phi t = h^{-1}\pi_K h$ (and remember that $\phi = \pi_J$). Without loss of generality, we can replace t by th so that $t^{-1}\phi t = \pi_K$.

Next, recall the matrices $A_J, A_K \in G(\mathbb{Q}_{(M)})$ which are congruent to the identity mod M and satisfy $A_J\pi A_J^{-1} = \pi_J$, $A_K\pi A_K^{-1} = \pi_K$. Therefore $t^{-1}A_J\pi A_J^{-1}t = A_K\pi A_K^{-1}$. It follows that $A_K^{-1}t^{-1}A_J$ commutes with π and therefore by Lemma 5.4 it is a polynomial in π with coefficients in $G(\mathbb{Q}_{(M)})$. In other words, for some $b \in L$, with (b) prime to M, $A_K^{-1}t^{-1}A_J = \tilde{b}$.

We have $w_\infty = A_{J,\infty}z_\infty$ for some cycle z_∞ in $X_\mathcal{O} = \overline{X_\infty^{\pi_\infty}}$. Then we have

$$\overline{w_\infty \tilde{y}_M t_l} = \overline{t_\infty^{-1} w_\infty t_M^{-1} \tilde{y}_M} = \overline{t_\infty^{-1} A_{J,\infty} z_\infty t_M^{-1} \tilde{y}_M} = \overline{A_{K,\infty}\tilde{b}_\infty z_\infty t_M^{-1} \tilde{y}_M} \equiv \overline{A_{K,\infty} z_\infty t_M^{-1} \tilde{y}_M},$$

where the congruence in means "homologous to." This is true because b_∞ is in the centralizer of π_∞ and therefore acts trivially on the homology of $X_\mathcal{O} \approx N_{\Gamma(M)}(\pi_\infty)\backslash X_\infty^{\pi_\infty} = Z_{\Gamma(M)}(\pi_\infty)\backslash X_\infty^{\pi_\infty}$.

On the other hand, we compute the action of E in this case:

$$\overline{w_\infty \tilde{y}_M}[\lambda_Q] = \overline{A_{J,\infty} z_\infty \tilde{y}_M}[\lambda_Q] = \overline{A_{Y,\infty} z_\infty \tilde{d}_M \tilde{y}_M}$$

where $Y \in \mathcal{R}$ and $d \in L$ such that in the absolute ideal class group we have $[\![Y]\!] = [\![J\lambda_Q]\!]$, and $(d) = YJ^{-1}\lambda_Q^{-1}$.

Let $B = B_\mathcal{O} A_J^{-1} = (b_1, \dots, b_n)$ be the basis we have fixed for J. Then we have the isomorphism $J/J\lambda_Q \approx \mathbb{Z}^n/t\mathbb{Z}^n$ given by $\sum \alpha_i b_i \mapsto (\alpha_i)$. It follows that

$$J\lambda_Q = Bt\mathbb{Z}^n = B_\mathcal{O} A_J^{-1} t\mathbb{Z}^n = B_\mathcal{O}\tilde{b}^{-1}A_K^{-1}\mathbb{Z}^n = \tilde{b}^{-1}B_\mathcal{O}A_K^{-1}\mathbb{Z}^n = \tilde{b}^{-1}K.$$

Therefore $[\![J\lambda_Q]\!] = [\![K]\!]$ and so $Y = K$ and $(d) = (b)$. Without loss of generality, we can take $d = b$.

We conclude that $\overline{A_{J,\infty} z_\infty \tilde{y}_M}[\lambda_Q] = \overline{A_{K,\infty} z_\infty \tilde{b}_M \tilde{y}_M}$. Finally since A_J and A_K are congruent to 1 mod M we have $t_M^{-1} \equiv b_M$ mod M. It follows that the right-hand side equals $\overline{A_{K,\infty} z_\infty t_M^{-1} \tilde{y}_M}$. Thus we have proved that $\overline{w_\infty \tilde{y}_M t_l} = \overline{w_\infty \tilde{y}_M}[\lambda_Q]$, and this finishes the proof of the theorem. □

Proof of Theorem 4.3. Let θ be given as in the theorem. Choose any nonzero element $\alpha_\mathcal{O}$ in the homology of $X_\mathcal{O}$. For example there certainly is one in H_0. Define $\alpha \in H_*(X_M)$ by $\alpha = \sum_{e\in E}\theta^{-1}(e)\alpha_\mathcal{O} e$. Then by Theorem 6.2,

$$\begin{aligned} \alpha T_s &= \sum_{Q\in\mathcal{I}} \alpha[\lambda_Q] = \sum_{e\in E}\sum_{Q\in\mathcal{I}} \theta^{-1}(e)\alpha_\mathcal{O} e[\lambda_Q] = \sum_{f\in E}\sum_{Q\in\mathcal{I}} \theta^{-1}\big(f\big[\lambda_Q^{-1}\big]\big)\alpha_\mathcal{O} f \\ &= \sum_{Q\in\mathcal{I}} \theta\big([\lambda_Q]\big)\alpha, \end{aligned}$$

where the equalities are all taken modulo $H_*^\beta(X)$. Since $H_*(X_M)$ is a direct summand in $H_*(X^{\pi_M})$, we are finished. □

References

[Ad] A. Adem, Automorphisms and cohomology of discrete groups, J. Algebra 182 (1996) 721–737.

[A] A. Ash, Galois representations attached to mod p cohomology of $GL(n,\mathbb{Z})$, Duke Math. J. 65 (2) (1992) 235–255.

[A1] A. Ash, Monomial Galois representations and Hecke eigenclasses in the mod-p cohomology of $GL((p-1)\mathbb{Z})$, Math. Ann. 315 (1999) 263–280.

[ADP] A. Ash, D. Doud, D. Pollack, Galois representations with conjectural connections to arithmetic cohomology, Duke Math. J. 112 (2002) 521–579.

[AS1] A. Ash, G. Stevens, Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues, J. Reine Angew. Math. 365 (1986) 192–220.

[AS] A. Ash, W. Sinnott, An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $GL(n,\mathbb{Z})$, Duke Math. J. 105 (2000) 1–24.

[BS] A. Borel, J.-P. Serre, Corners and arithmetic groups, Comm. Math. Helv. 48 (1973) 436–491.

[B] G. Bredon, Introduction to Compact Transformation Groups, Academic Press, New York, 1972.

[B1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over Q, J. Amer. Math. Soc. 14 (2001) 843–939.

[Br] K. Brown, Cohomology of Groups, Springer-Verlag, New York, 1982.

[CR] C. Curtis, I. Reiner, Methods of Representation Theory, Vol. 1, Wiley–Interscience, New York, 1981.

[Se] J.-P. Serre, Sur les representations modulaires de degre 2 de $\mathrm{Gal}(\overline{Q}/Q)$, Duke J. 54 (1987) 179–230.

[S-BT] N. Shepherd-Barron, R. Taylor, Mod 2 and mod 5 icosahedral representations, J. Amer. Math. Soc. 10 (1997) 283–298.

[T1] R. Taylor, Remarks on a conjecture of Fontaine and Mazur, J. Inst. Math. Jussieu 1 (2002) 1–19.

[T2] R. Taylor, On icosahedral Artin representations II, Amer. J. Math., to appear.